

**NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT  
VERSION (2019)**

**Concord School District**

**and**

**EBSCO Publishing, Inc.**

**October 13, 2020**

This New Hampshire Student Data Privacy Agreement (“DPA”) is entered into by and between Concord School District (hereinafter referred to as “LEA”) and EBSCO Publishing, Inc. (hereinafter referred to as “Provider”) on October 13, 2020. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS**, , the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

**WHEREAS**, the Provider may, by signing the “General Offer of Privacy Terms” in Exhibit “E”, agree to allow other school districts in New Hampshire the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA; and

**WHEREAS**, in order to provide the Services described in the Services Agreement and in Article 1 and Exhibit “A” of this DPA, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232hand the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

**WHEREAS**, the documents and data transferred from New Hampshire LEAs and created by the Provider’s Services may also subject to several New Hampshire student privacy laws, including RSA 189:65-68-a, RSA 186-C; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, for the purposes of this DPA, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) is transmitted to Provider from LEA, the Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Services Agreement; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

## ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to the Services Agreement, including compliance with all applicable privacy statutes, which may include the FERPA, PPRA, COPPA, IDEA, RSA 189:65 through 68-a, 186-C (where applicable) NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) is transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided.** The Provider has agreed to provide the digital educational products and services described in Exhibit “A”.
3. **Student Data to Be Provided.** In order to perform the Services pursuant to the Services Agreement and as described in this Article and Exhibit “A”, LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit “B”.
4. **DPA Definitions.** The definitions of terms used in this DPA are found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Services Agreement and all other writings, including, but not limited to, privacy policies or any terms of service.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to the Services Agreement and this DPA is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of the Services Agreement and this DPA in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Services Agreement and this DPA shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. The Provider will cooperate and provide Student Data within fourteen (14) days at the LEA’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information in the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall cooperate and respond in a timely manner (and no later than 14 days from the date of the request) to the LEA’s request for Personally Identifiable Information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records or Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Services Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Services.

4. **Third Party Request.** Unless legally prohibited, should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. Except with respect to Student Data accessed by or disclosed or transferred to Subprocessors in connection with providing the Services, the Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.
5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Services Agreement and this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Services Agreement and this DPA, whereby the Subprocessors agree to protect Student Data in manner similar with the terms of this DPA.

### **ARTICLE III: DUTIES OF LEA**

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the Services Agreement and this DPA in compliance with, as applicable, the FERPA, PPRa, COPPA, IDEA, RSA 189:65 through 68-a RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### **ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** The Provider shall comply with all applicable New Hampshire and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRa, IDEA, RSA 189:65 through 68-a; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.
2. **Authorized Use.** Student Data shared pursuant to the Services Agreement and this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Services Agreement and this DPA, and as authorized under the statutes referred to in subsection (1), above. Except as authorized in this DPA and/or the statutes referred to in subsection (1) above, Provider also acknowledges and agrees that it shall not make any re-

disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or Personally Identifiable Information contained in the Student Data, without the express written consent of the LEA, unless there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Services Agreement and this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data.
4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless that party agrees in writing not to attempt re-identification and notice has been given to the LEA who has provided prior written consent for such transfer. Notwithstanding the foregoing, Provider may transfer Student Data, including de-identified Student Data, to the approved list of Subprocessors included in Exhibit A in connection with providing the Services to LEA. For the avoidance of doubt, Provider shall provide advance notice of any changes to its list of Subprocessors included in Exhibit A. For purposes of clarification, information is only shared with Subprocessors in the course of service delivery in support of the Services. Provider shall not copy, reproduce or transmit any data obtained under the Services Agreement and this DPA and/or any portion thereof, except as necessary to fulfill the Services Agreement and this DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which de-identified data is presented.
5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in this paragraph, Provider shall dispose or delete all Personally Identifiable Information obtained under the Services Agreement and this DPA when it is no longer needed for the purpose for which it was obtained and, if applicable, transfer said data to LEA or LEA’s designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Notwithstanding the foregoing, archive/backup data is excluded from this, and is treated as production data until its destruction. Provider will notify the LEA within thirty (30) days of restoring any of the LEA’s data from its back-up systems. The LEA may request deletion of any restored LEA data.

Nothing in the Services Agreement or this DPA authorizes Provider to maintain Personally Identifiable Information obtained under the Services Agreement and this DPA beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) erasing; or (3) otherwise modifying the Personally Identifiable Information in those records to make it unreadable or indecipherable. Upon request, Provider shall provide written notification to LEA when the Personally Identifiable Information has been disposed. The duty to dispose of Personally Identifiable Information shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of this DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

6. **Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Services to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Services to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

## **ARTICLE V: DATA PROVISIONS**

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. These measures shall include, but are not limited to:
  - a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
  - b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Information contained in Student Data and obtained under the Services Agreement and this DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Services Agreement or this DPA authorizes Provider to maintain Personally Identifiable Information beyond the time period reasonably needed to complete the disposition.
  - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Services Agreement and this DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Services Agreement and this DPA, except as necessary to provide Services to LEA and to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in the Services Agreement or this DPA.
  - d. **Employee Training.** The Provider shall provide recurring, periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
  - e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall offer the LEA the ability to enable or disable Secure Socket Layer (“SSL”) or equivalent technology to protect data from unauthorized access through the EBSCO

admin interface. The service security measures shall include server authentication and data encryption when enabled by the LEA. Provider shall host data pursuant to the Services Agreement and this DPA in an environment using a firewall that is periodically updated according to industry standards.

- f. Security Coordinator.** If different from the designated representative identified in Article VI, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Services Agreement and this DPA.
- g. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- h. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
- i. Audits.** At least once a year, and upon request the Provider will provide a copy of the ISO 27001 certification (expected in fall 2020). The Provider will cooperate reasonably with any state or federal agency with oversight authority/jurisdiction in connection with any investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to resources with appropriate subject matter knowledge and to LEA's Student Data.
- j. New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. Specifically, the Provider agrees to:
  - i.** Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - ii.** Limit unsuccessful logon attempts;
  - iii.** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - iv.** Authorize wireless access prior to allowing such connections;
  - v.** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - vi.** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - vii.** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - viii.** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

- ix. Enforce a minimum password complexity and change of characters when new passwords are created;
- x. Perform maintenance on organizational systems;
- xi. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- xii. Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1;
- xiii. Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;
- xiv. Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- xv. Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas;
- xvi. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- xvii. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- xviii. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception); Protect the confidentiality of Student Data at rest;
- xix. Identify, report, and correct system flaws in a timely manner;
- xx. Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- xxi. Monitor system security alerts and advisories and take action in response; and
- xxii. Update malicious code protection mechanisms when new releases are available.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and no later than within ten (10) days of Provider becoming aware of the incident. Provider shall follow the following process:

- a. The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “When it Occurred,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
  - i. The name and contact information of the reporting LEA subject to this section.



- ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
  - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - vi. The estimated number of students and teachers affected by the breach, if any.
- c. At LEA’s discretion, the security breach notification may also include any of the following:
- i. Information about what the agency has done to protect individuals whose information has been breached.
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Provider agrees to adhere to all requirements in the New Hampshire Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, and agrees to make staff available at reasonable times to answer questions of the LEA on the written incident plan. .
- f. If LEA requests Provider’s assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

## ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA so long as the Provider maintains any Student Data.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as the Services Agreement has lapsed or has been terminated. LEA may terminate this DPA and the Services Agreement if the Provider materially breaches any terms of this DPA.
3. **Effect of Termination Survival**. If the Services Agreement is terminated, the Provider shall destroy all of LEA’s data pursuant to Article V, section 1(b).

4. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA, IDEA, COPPA PPRRA, RSA 189:65-68a;; RSA 186-C; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of the DPA and any other writing, such as the Services Agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.
  
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name \_\_\_\_\_  
 Title \_\_\_\_\_  
 Address EBSCO Information Services  
10 Estes Street, Ipswich, MA 01938  
 Telephone 800-653-2726  
 Email \_\_\_\_\_

The designated representative for the LEA for this DPA is:

Pam McLeod, CETL  
 Director of Technology | Concord School District  
 38 Liberty Street, Concord, NH 03301  
 (603) 225.0811 | pmcleod@sau8.org

6. **Entire Agreement.** This DPA, along with the Services Agreement and the Provider’s Privacy Policy and Terms of Use constitute the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
  
7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without

invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF MERRIMACK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and/or any portion thereof are stored, maintained or used in any way.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This DPA may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this DPA. In proving this DPA, it shall not be necessary to produce or account for more than one such counterpart.

## ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other school district who signs the acceptance in said Exhibit. The Form of General Offer of Privacy Terms is limited by the terms and conditions described therein.

*[Signature Page Follows]*

IN WITNESS WHEREOF, the parties have executed this New Hampshire Student Data Privacy Agreement as of the last day noted below.

**CONCORD SCHOOL DISTRICT**

By:  Pamela McLeod (Oct 16, 2020 13:09 EDT) Date: 10/16/2020

Printed Name: Pamela R McLeod Title/Position: Director of Technology

**EBSCO PUBLISHING, INC.**

By:  Date: 10/16/2020

Printed Name: Alex Saltzman Title/Position: Sr. VP, Inside Sales

**EXHIBIT “A”**  
**DESCRIPTION OF SERVICES**

EBSCO is providing subscription-based access to the following database products\*:

EBSCO databases, ABC CLIO databases, Flipster, EBSCO Discovery Service, EBSCO eBooks

\*This DPA assumes the LEA accesses EBSCO databases through the Explora or Reference Center interfaces; or, if using the EBSCOhost or EBSCO Discovery Service interfaces, that the folder personalization feature is not enabled.

**Subprocessor List**

Provider will not add new Subprocessors without getting prior approval.

Name	Description	(Category of) Personal Data processed by the Sub-processor	Country of Processing	Country where Sub-processor's registered office is located
<b>Amazon Web Services (AWS)</b>	Software delivery platform and hosting services	First Name, Last Name, Email Address, Password and UserID	United States	United States
<b>Auth0</b>	Federated identity for EBSCO products	First Name, Last Name, Email Address, Password and UserID	United States	United States
<b>CyberSource</b>	Credit card processing	Not Applicable	United States	United States
<b>Google-Auth</b>	3rd-party federated identity - NO PD SHARED	Not Applicable	United States	United States
<b>Google-Classroom</b>	K-12 classroom management - NO PD SHARED	Not Applicable	United States	United States
<b>Marketo</b>	Marketing campaign management	Not Applicable	United States	United States
<b>NES</b>	First Line Customer Support	First Name, Last Name, Email Address, Password and UserID	India	India
<b>NetSuite</b>	CRM for customer interactions about products	Not Applicable	United States	United States
<b>OpenAthens</b>	Academic 3rd party federated identity	First Name, Last Name, Email Address, Password and UserID	United States	United States
<b>SalesForce</b>	CRM for customer interactions about products	Not Applicable	United States	United States

<b>Shibboleth</b>	Academic 3rd party federated identity	First Name, Last Name, Email Address, Password and UserID	United States	United States
<b>Stripe</b>	Credit card processing	Not Applicable	United States	United States
<b>Tufts Continuing Medical Education</b>	Management of medical continuing ed credits		United States	United States
<b>Baylor</b>	Management of medical continuing ed credits		United States	United States

## EXHIBIT “B”

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	X Data deidentified, Journal/Title level information only in compliance with Counter5 Standard (projectcounter.org)
Assessment	Standardized test scores	
	Observation data	
	Other assessment data- Please specify:	
-	-	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
-	-	
Communications	Online communications that are captured (emails, blog entries)	
-	-	
Conduct	Conduct or behavioral data	
-	-	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information- Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	

Category of Data	Elements	Check if used by your system
	Other enrollment information- Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
-	-	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
-	-	
Parent/Guardian Name	First and/or Last	
-	-	
Schedule	Student scheduled courses	
	Teacher names	
-	-	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information- Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	X Over 13 years old only
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Student In-App Performance	Program/application performance (typing program student types 60 wpm, reading program student reads below grade level)	
-	-	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
-	-	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	X
	Other student work data – Please specify:	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data – Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
-	-	
Other	Please list each additional data element used, stored or collected by your application	



## EXHIBIT “C”

### DEFINITIONS

**De-Identifiable Information (DI):** De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

**NIST 800-63-3:** Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

**Personally Identifiable Information (PII):** The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address
Unique pupil identifier	
Credit card account number, insurance account number, and financial services account number	
Name of the student's parents or other family members	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email

**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

**Pupil Generated Content:** The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

**Services Agreement:** Refers to the contract or license agreement to which this DPA supplements and modifies.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, the name of the student’s parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this DPA, and for the purposes of New Hampshire and federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

**Subscribing LEA:** An LEA that was not a party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

**Subprocessor:** For the purposes of this DPA, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other services to operate and/or improve its products and services, and who has access to PII.

**Targeted Advertising:** Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

**Third Party:** The term “Third Party” means an entity that is not the Provider or LEA.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

[Name or District or LEA] ("LEA") directs EBSCO Publishing, Inc. ("Provider") to dispose of data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the disposition are set forth below:

1. Extent of Disposition

\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

\_\_\_ As soon as commercially practicable

\_\_\_ By (Insert Date)

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Provider

\_\_\_\_\_  
Date

**OPTIONAL: EXHIBIT “F”**

**DATA SECURITY REQUIREMENTS**

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy?  Yes  No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

\_\_\_ ISO 27001/27002

\_\_\_ CIS Critical Security Controls

\_\_\_ NIST Framework for Improving Critical Infrastructure Security

\_\_\_ Other: \_\_\_\_\_

3. Does your organization store any customer data outside the United States?  Yes  No

4. Does your organization encrypt customer data both in transit and at rest?  Yes  No  Custom

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: John Graham

Contact information: jwgraham@ebSCO.com

6. Please provide any additional information that you desire.

**See attached Security White Paper.**

**White Paper: Information Security Practices**

**Introduction**

Information Security (IS) is a priority at EBSCO Information Services (EBSCO). Our mission is to incorporate security and risk management practices into our policies, procedures, and day-to-day operations within the organization. This approach enables appropriate diligence to ensure adequate protection of information assets and systems.